REMARKS

Claims 1-3, 5-12 and 14-27 are presently pending in the above-identified application. Claims 1, 2, 5-11, 14-16, 18-25 and 27 are proposed to be amended herein.

Rejection of Claims under 35 USC § 102

The Office Action rejected claims 1-3, 5-12 and 15-27 as being anticipated by U.S. Patent No. 6,298,445 issued to A. Shostack et al. (hereinafter "Shostack"). Applicants have amended the claims herein to more particularly claim the various aspects of the invention, and respectfully submit that each of the currently pending is patentably distinct from Shostack.

To be clear, the Applicants recognize that "spoofing", i.e., the faking of the sending address of a transmission in order to gain illegal entry into a secure system (see, e.g., a general definition available at http://www.techweb.com/encyclopedia; or Shostack at column 1, line 64 – column 2, line 3) is not new. Indeed, Applicant William Cheswick in the subject Application is a recognized Internet security expert (see, e.g., the enclosed references) intimately familiar with spoofing and spoofed packets. Heretofore, the well-known use of spoofed packets (by unauthorized users or hackers) is directed to gaining illegal entry into a secure system. In contrast, Applicants have realized that spoofed packets can serve different purposes (and non-malicious) by providing an enhanced security tool for discovering the connectivity between networks. This connectivity measure, in turn, can be used by system administrators to prevent malicious attacks (including but not limited to malicious spoofing). It is at least this aspect of Applicants' invention that stands in stark contrast to the cited prior art.

More particularly, in accordance with an aspect of the invention, certain information, which defines a particular communications network, is utilized to make a determination with respect to the connectivity of the hosts within the network. That is, in accordance with an aspect of the invention, the perimeter of the communications network is analyzed as a function of a census of such communications thereby identifying particular host(s) within the network and routes associated thereto. A security characteristic of the host (or hosts) associated with a first communications network is

analyzed wherein the security characteristic is a measure of connectivity between the first communications network and a second communications network. That is, the host is probed with a particular packet, where the packet includes a source address which is associated with the second communications network, and the connectivity measure is determined as function of a response from the probed host (see, e.g., Applicants' Specification, page 4, line 27 – page 5, line 6; and page 8, lines 20-22).

Advantageously, Applicants' have realized that using the so-called "spoofed probe packet" (see, e.g., Applicants' Specification, page 9, lines 17-20 and lines 21-23) the connectivity of certain hosts can be measured and such connectivity measure can be used to identify potential unsecure or "rogue" connections between the probed host and some other host on the second communications network (see, e.g., Applicants' Specification, page 10, lines 5-7). The probe packet, in accordance with this aspect of the invention, is not used for malicious purposes in gaining illegal entry into the first or second communications network—but rather—for non-malicious purposes in providing an enhanced security tool for discovering the connectivity between networks.

To that end, Applicants have amended the originally filed claims to more particularly claim the above-described aspect of the invention. For example, amended independent claims 1 recites:

> "...probing at least one host of the plurality hosts of the first communications network by transmitting a packet to the host, the host being selected from the census results and the packet having at least a source address which is associated with a second communications network; and
>
> determining a security characteristic of the probed host as a function of a response by the probed host in receiving the packet, the security characteristic being a measure of connectivity between the first communications network and the second communications network." (Emphasis added by Applicants)

Each of the currently pending claims has been amended in a similar fashion as the above-referenced amended claim 1 to more particularly claim this aspect of the invention.

Applicants appreciate how the Examiner may have found certain similarities between Shostack and Applicants' originally filed claims. However, as mentioned above, Applicants respectfully submit that the amended claims herein are patentably distinct from Shostack. More particularly, Applicants' understand Shostack to teach a computer security system directed to providing real-time updates which provide updated information related to so-called "security vulnerabilities" (see, Shostack, column 1, lines 31-43). Further, Shostack's security system provides for a so-called "network security detector" which monitors security intrusions on a network (see, Shostack, column 1, lines 61-65). Shostack's teaching with regard to "IP spoofing" (see, e.g., column 1, line 64 – column 2, line 3; and column 4, lines 52-57) is consistent with the known prior art spoofing as highlighted above by Applicants.

However, Applicants find no teaching or suggestion in Shostack with respect to the aspect of Applicants' claimed invention directed to utilizing a spoofed probe packet to determine a connectivity measure between two communication networks which can be used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and some other host on a second communications network, as detailed above. As such, in view of the foregoing, Applicants respectfully submit that each of the currently pending independent claims, as amended, are patentably distinct from Shostack.

Regarding the rejection of each of the presently pending dependent claims, as amended, these claims depend ultimately from one of the pending amended independent claims 1, 10, 16, 21 and 24 herein which Applicants submit are patentably distinct over Shostack for the aforesaid reasons. Thus, these dependent claims contain all the limitations of the pending amended independent claims from which they depend, and Applicants respectfully submit that these dependent claims are also patentably distinct over Shostack for the aforesaid reasons, as well as other elements these claims add in combination to their base claim.

Rejection of Claims under 35 USC § 103(a)

The Office Action rejected claims 4 and 13 under 35 USC § 103(a) as being unpatentable over Shostack, and rejected claim 14 as being unpatentable over Shostack in view of U.S. Patent No. 6,212,561 issued to Sitaraman et al. (hereinafter "Sitaraman"). In view of the cancellation of originally filed dependent claim 4 and 13 the aforementioned rejection of such claims is deemed moot.

Regarding dependent claim 14, as amended, and each of the other pending claims herein, Applicants respectfully submit that nothing in Shostack or Sitarman taken alone or in any combination teaches or suggests the various aspects of Applicants' invention as claimed herein.

More particularly, combining the teaching of Sitarman would provide Shostack's security system with the further feature of forced sequential access thereby forcing authorized users in Shostack's system to disconnect from any open connections to other public or private domains or networks before a connection with the user's domain can be established (see, e.g., Sitarman, column 4, lines 36-41). Nothing in the Shostack/Sitarman combination teaches or suggests utilizing a spoofed probe packet to determine a connectivity measure between two communication networks which can be used to identify potential unsecure or rogue connections between a probed host (of a first communications network) and some other host on a second communications network, as detailed above

In view of the foregoing, it is respectfully submitted that each of the currently pending claims in the application is in condition for allowance and reconsideration is requested. Favorable action is respectfully requested.

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact the undersigned at the telephone number listed below.

Respectfully submitted,

Steven Branigan
Hal Joseph Burch
William R. Cheswick

By _____
Donald P. Dinella
Attorney for Applicants
Reg. No. 39,961
908-582-8582

Date: April 7, 2004

Docket Administrator (Room 3J-219)
Lucent Technologies Inc.
101 Crawfords Corner Road
Holmdel, NJ 07733-3030

Enclosures:
Copy of TechTV (www.techtv.com) excerpt
Copy of Computerworld (www.computerworld.com) excerpt